Amendments to the Claims

The listing of claims presented below replaces all prior versions, and listings, of claims in the application.

Listing of claims:

1. (currently amended) A method for securely encoding and transmitting a message by an originating device ~~of a secure message~~ to one of a plurality of recipient devices, said message being associated with a particular one of a plurality of applications running on the originating device, the method comprising the steps of:

(a) determining a device identifier for the originating device, and an application identifier for each of the plurality of applications thereby forming a plurality of device-identifier/application identifier pairs;

(b) associating a secret value with each device-identifier/application-identifier pair;

(c) wherein each said secret value is known to the originating device and to one of the recipient devices;

[[(a)]] (d) generating a message value by a first process ~~using a~~ , using the device identifier, [[an]] a particular application identifier and an application value a ~~message value~~ , said application value indexing said message;

[[(b)]] (e) combining the message value with ~~one or more first secret values, said secret values being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value~~ said secret value associated with the particular application identifier to establish a corresponding secret message value;

[[(c)]] (f) applying the secret message value and the message to an encoding process to form a secure message block; and

[[(d)]] (g) combining ~~an address with~~ the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable, dependent upon the device identifier, the particular application identifier and the application value which are outside the received secure message block, by ~~the one or more of~~ said ~~intended~~ recipient ~~devices which~~ device to which said secret value associated with

the particular application identifier is known, said recipient device thereby ~~recover~~ recovering the message, ~~the address~~, the device identifier, the particular application identifier and the application value.

2. (currently amended) A method according to claim 1, ~~whereby~~ wherein an association of the device identifier, the application identifier, and the application value substantially uniquely identifies the originating device and a purpose of one or more of the message and the application, and establishes an identifier for the message, ~~such~~ said message ~~identification~~ identifier being bound with the message content by virtue of the encoding process.

3. (currently amended) A method according to claim 1, ~~whereby~~ wherein the encoding process in step [[(c)]] (f) comprises one or more of:

[[(e)]] a symmetric encryption process;

[[(f)]] an integrity process using one of keyed hash and symmetric encryption techniques;

[[(g)]] a process including both symmetric encryption and keyed integrity; and

[[(h)]] including the secret message value in a higher level messaging protocol.

4. (currently amended) A method for reception of a securely transmitted message by a recipient device, the recent device being one of a plurality of recipient devices adapted to receive a message from an originating device, said message being associated with a particular one of a plurality of applications running on the originating device, the method comprising the steps of:

(i) extracting one or more of a device identifier, an application identifier and an application value from a received secure message having a secure message block, said one or more of the device identifier, the application identifier, and the application value being outside the secure message block, said application value indexing said message;

(j) generating by a first process using the device identifier, the application identifier and the application value a message value;

(k) generating, according to a second process using the device identifier and the application identifier ~~one or more secret values~~ a secret value known ~~substantially~~ only to [[an]] the originating device and the ~~one or more intended~~ recipient ~~devices of the message~~ device;

(l) combining the message value with the ~~one or more~~ secret ~~values~~ value, to establish a secret message value;

(m) extracting a secure message block from the received secure message; and

(n) applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device.

5 - 13. (cancelled)

14. (new) An originating device for securely encoding and transmitting a message to one of a plurality of recipient devices, the message being associated with a particular one of a plurality of applications running on the originating device, the originating device comprising:

(a) means for determining a device identifier for the originating device, and an application identifier for each of the plurality of applications thereby forming a plurality of device-identifier/application identifier pairs;

(b) means for associating a secret value with each device-identifier/application-identifier pair;

(c) wherein each said secret value is known to the originating device and to one of the recipient devices;

(d) means for generating a message value by a first process, using the device identifier, a particular said application identifier and an application value said application value indexing said message;

(e) means for combining the message value with a said secret value associated with the particular application identifier to establish a corresponding secret message value;

(f) means for applying the secret message value and the message to an encoding process to form a secure message block; and

(g) means for combining the device identifier the particular application identifier the application value and the secure message block to form a secure message for transmission, said secure message being decodable, dependent upon the device identifier the particular application identifier and the application value which are outside the received secure message block, by a said recipient device to which said secret value associated with the particular application identifier is known, said recipient device thereby recovering the message, the device identifier, the particular application identifier and the application value.

15. (new) Apparatus according to claim 14, wherein the encoding means comprises one or more of:

(e) a symmetric encryption means;

(f) an integrity processing means using keyed hash or symmetric encryption techniques;

(g) a keyed-symmetric processing means performing symmetric encryption and ensuring keyed integrity; and

(h) encapsulation means for including the secret message value in a higher level messaging protocol.

16. (new) A computer program product according to claim 15, whereby the encoding steps in step (f) comprise one or more of:

symmetric encryption steps;

integrity processing steps using one of keyed hash and symmetric encryption techniques;

keyed-symmetric steps performing symmetric encryption and ensuring keyed integrity; and

encapsulation steps for including the secret message value in a higher level messaging protocol.

17. (new) A computer program product including a computer readable medium having recorded thereon a computer program for directing an originating device to securely encode and transmit a secure message to one of a plurality of recipient

devices, said message being associated with a particular one of a plurality of applications running on the originating device, the program comprising:

(a) code for determining a device identifier for the originating device and an application identifier for each of the plurality of applications thereby forming a plurality of device-identifier/application identifier pairs;

(b) code for associating a secret value with each device-identifier/application-identifier pair;

(c) wherein each said secret value is known to the originating device and to a said one of the recipient devices;

(d) code for generating a message value by a first process, using the device identifier, a particular said application identifier and an application value said application value indexing said message;

(e) code for combining the message value with said secret value associated with the particular application identifier to establish a corresponding secret message value;

(f) code for applying the secret message value and the message to an encoding process to form a secure message block; and

(g) code for combining the device identifier the particular application identifier the application value and the secure message block to form a secure message for transmission, said secure message being decodable, dependent upon the device identifier the particular application identifier and the application value which are outside the received secure message block, by said recipient device to which said secret value associated with the particular application identifier is known, said recipient device thereby recovering the message, the device identifier, the particular application identifier and the application value.

18. (new) A recipient device for reception of a securely transmitted message, the recipient device being one of a plurality of recipient devices adapted to receive a message from an originating device, said message being associated with a particular one of a plurality of applications running on the originating device, the recipient device comprising:

(i) means for extracting one or more of a device identifier, an application identifier and an application value from a received secure message having a secure

message block, said one or more of the device identifier, the application identifier, and the application value being outside the secure message block, said application value indexing said message;

(j) means for generating by a first process using the device identifier, the application identifier and the application value a message value;

(k) means for generating, according to a second process using the device identifier and the application identifier a secret value known only to the originating device and the recipient device;

(l) means for combining the message value with the secret value, to establish a secret message value;

(m) means for extracting a secure message block from the received secure message; and

(n) means for applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device.

19. (new) A computer program product including a computer readable medium having recorded thereon a computer program for directing a recipient device to process a received secure message, the recipient device being one of a plurality of recipient devices adapted to receive a message from an originating device, said message being associated with a particular one of a plurality of applications running on the originating device, the program comprising:

(i) code for extracting one or more of a device identifier, an application identifier and an application value from a received secure message having a secure message block, said one or more of the device identifier, the application identifier, and the application value being outside the secure message block, said application value indexing said message;

(j) code for generating by a first process using the device identifier, the application identifier and the application value a message value;

(k) code for generating, according to a second process using the device identifier and the application identifier a secret value known only to the originating device and the recipient device;

(l) code for combining the message value with the secret value, to establish a secret message value;

(m) code for extracting a secure message block from the received secure message; and

(n) code for applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device.

20. (new) A system providing secure communications, the system comprising an originating device and one or more receiving devices, wherein:

said originating device is adapted for securely encoding and transmitting a message to one of a plurality of recipient devices, the message being associated with a particular one of a plurality of applications running on the originating device, the originating device comprising:

(a) means for determining a device identifier for the originating device, and an application identifier for each of the plurality of applications thereby forming a plurality of device-identifier/application identifier pairs;

(b) means for associating a secret value with each device-identifier/application-identifier pair;

(c) wherein each said secret value is known to the originating device and to one of the recipient devices;

(d) means for generating a message value by a first process, using the device identifier, a particular said application identifier and an application value, said application value indexing said message;

(e) means for combining the message value with a secret value associated with the particular application identifier to establish a corresponding secret message value;

(f) means for applying the secret message value and the message to an encoding process to form a secure message block; and

(g) means for combining the device identifier, the particular application identifier, the application value and the secure message block to form a secure message for transmission, said secure message being decodable, dependent upon the device identifier, the particular application identifier and the application value

which are outside the received secure message block, by said recipient device to which said secret value associated with the particular application identifier is known, said recipient device thereby recovering the message, the device identifier, the particular application identifier and the application value; and wherein;

said recipient device is adapted for reception of a securely transmitted message, the recipient device being one of the plurality of recipient devices adapted to receive a message from the originating device, said message being associated with a particular one of a plurality of applications running on the originating device, the recipient device comprising:

(h) means for extracting one or more of a device identifier, an application identifier and an application value from a received secure message having a secure message block, said one or more of the device identifier, the application identifier, and the application value being outside the secure message block;

(i) means for generating by a first process using the device identifier, the application identifier and the application value a message value;

(j) means for generating, according to a second process using the device identifier and the application identifier a secret value known only to the originating device and the recipient device;

(k) means for combining the message value with the secret value, to establish a secret message value;

(l) means for extracting a secure message block from the received secure message; and

(m) means for applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device.

21. (new) A system according to claim 20;

wherein said originating device comprises:

(n) first processing means;

(o) transmitting means adapted to perform one or more establishing and maintaining communications with a receiving means, said first processing means being adapted to control said transmitting means, and adapted to support features (a) to (g);

wherein said receiving device comprises:

(p) second processing means; and

(q) the receiving means, being adapted to perform one or more of establishing and maintaining communications in conjunction with said transmitting means, said second processing means being adapted control said receiving means, and further adapted to support features (h) to (m).

22. (new) A system according to claim 21, wherein said originating device comprises one of:

(r) a PC comprising the transmitting means, a smart card reader, the first processing means being responsive to the smart card reader and adapted to control said transmitting means, said originating device further comprising a smart card adapted to interface with the smart card reader, said smart card having on board second processing means which in conjunction with said first processing means are adapted to support features (a) to (g); and

(s) a mobile telephone, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (g); and

(t) a set top box, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (g); and

(u) a cable modem, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (g); and

(v) a personal digital assistant, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (g).

23. (new) A method for reception according to claim 4, wherein:

a plurality of applications are running on the recipient device; and

the application identifier extracted in the extracting step (i) is used to identify one of the applications running on the recipient device, said identified application being adapted to process the securely transmitted message decoded in step (n).